

STATE OF GEORGIA
HENRY COUNTY
CITY OF STOCKBRIDGE

RESOLUTION NO. R20-1139

**A RESOLUTION TO ADOPT A POLICY WITH RESPECT TO
INFORMATION TECHNOLOGY**

WHEREAS, the City of Stockbridge ("City") is a municipal corporation duly organized and existing under the laws of the State of Georgia and is charged with being fiscally responsible concerning the use and expenditure of all public funds; and

WHEREAS, the City Council desires to establish a policy with respect to Information Technology;

THEREFORE, THE CITY COUNCIL OF THE CITY OF STOCKBRIDGE HEREBY RESOLVES:

SECTION 1. Approval. The policy attached hereto as Exhibit A is hereby approved.

SECTION 2. Public Record. This document shall be maintained as a public record by the City Clerk and shall be accessible to the public during all normal business hours of the City of Stockbridge.

SECTION 3. Authorization of Execution. The Mayor or Mayor Pro Tem is hereby authorized to sign all documents necessary to effectuate this Resolution.

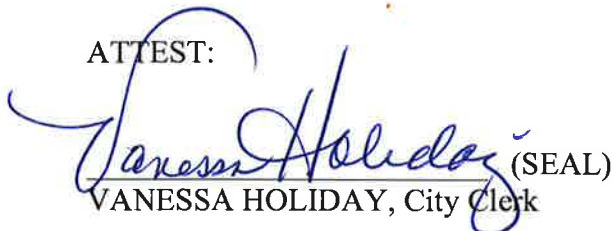
SECTION 4. Attestation. The City Clerk is authorized to execute, attest to, and seal any documents which may be necessary to effectuate this ordinance, subject to approval as to form by the City Attorney.

SECTION 5. Effective Date. This resolution shall become effective immediately upon its adoption by the Mayor and City Council of the City of Stockbridge as provided in the City Charter.

SO REOLVED this 28th day of January, 2020.


ANTHONY S. FORD, Mayor

ATTEST:

 (SEAL)
VANESSA HOLIDAY, City Clerk

APPROVED AS TO FORM:

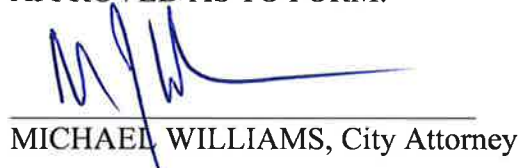

MICHAEL WILLIAMS, City Attorney

EXHIBIT A

INFORMATION TECHNOLOGY POLICY

City of Stockbridge, General IT Policy

Purpose: The intent of the Technology Usage Policy is to define the acceptable use of technology at the City of Stockbridge and to ensure that the City complies with all legally mandated requirements. It outlines the responsibilities of those who work for and on behalf of the City in contributing to the maintenance and protection of its information resources in a secure, stable and cost-effective manner.

Policy Scope: The City of Stockbridge's Technology Usage Policy defines the oversight, use and protection of the City of Stockbridge's computing equipment, network, voice, electronic communications and data repositories. This includes the acquisition, access and use of all software, hardware and shared resources, whether connected to the network, configured off the network, or while in transit (mobile). It applies to all those who work on behalf of the City of Stockbridge including, but not limited to, employees, contractors, consultants, temporaries, supplementals, intern's, volunteers and other workers including all personnel affiliated with third parties. This policy also applies to all equipment that is owned or leased by the City regardless of project and program funding sources.

Use of computers

- Only the employees of the City of Stockbridge and other designated persons are authorized to use or access the department's computers.
- Employees will only use computer software and related equipment in the direct performance of their assigned duties unless authorized by their department head.
- Employees needing assistance with computer related problems should contact the IT Department either by phone, email or submit a computer work order for all hardware or software problems and installations.
- Use of Company computers, networks, and Internet access is a privilege granted by the administration and may be revoked at any time for inappropriate conduct carried out on such systems, including, but not limited to:
 - Sending chain letters or participating in any way in the creation or transmission of unsolicited commercial e-mail ("spam") that is unrelated to legitimate City purposes;
 - Engaging in private or personal business activities, including instant messaging and chat rooms or listening to the radio
 - Misrepresenting oneself or the City;
 - Violating the laws and regulations of the United States or any other nation or any state, city, province, or other local jurisdiction in any way;
 - Engaging in unlawful or malicious activities;
 - Deliberately propagating any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either the Company's networks or systems or those of any other individual or entity;

- Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages;
- Sending, receiving, or accessing pornographic materials;
- Becoming involved in partisan politics;
- Causing congestion, disruption, disablement, alteration, or impairment of the City networks or systems;
- Maintaining, organizing, or participating in non-work-related Web logs ("blogs"), Web journals, "chat rooms", or private/personal/instant messaging;
- Failing to log off any secure, controlled-access computer or other form of electronic data system to which you are assigned, if you leave such computer or system unattended;
- Using recreational games; and/or
- Defeating or attempting to defeat security restrictions on company systems and applications.

Email Communication

- The electronic mail system is intended for business purposes. Electronic mail communications constitute public records and the City has the right to access or monitor messages for work-related purposes, security, or to respond to public record requests. All messages should be composed with the expectation that they are public. Refrain from using your City email address for anything other than official business.
- Users shall have no expectation of privacy in email messages, whether they are business related or an allowed personal use as provided herein. Use of electronic mail shall be considered consent to City Officials, managers, and other employees to inspect, use, or disclose any electronic mail or other electronic communications and/or data.
- Use of Non-City Email Accounts-Non-City email accounts (like MSN, Yahoo!, Gmail, Hotmail, etc.) may not be used to conduct City business. Likewise, a non-City email account may not be forwarded to a City email account.
- Transmission of Confidential Information-Confidential material must not be sent via electronic mail. Electronic mail messages may be intercepted, viewed, and used for non-approved purposes, especially when corresponding via the Internet, a medium over which the City has no control.
- E-mail communications will conform to the same professional standards as with written and verbal business correspondence. A professional tone should prevail, and content will be consistent with and representative of the City's policies and practices.

- Any attempt to misrepresent one's identity via e-mail is prohibited.
- E-mail is considered part of the public record and is subject to disclosure under Georgia State law. Managing individual e-mail storage and retention is the responsibility of each department, consistent with document and records-retention guidelines. Effort should be made to restrict unnecessary e-mail traffic, including minimizing the size of attachment files; and using network drives instead of large distribution lists to share file attachments with large groups.
- Any emails sent that have customer identifier information (Address, social security number, le) Must be encrypted internally and externally.

Use of software

- No downloaded application software is to be installed on any City equipment by anyone except the IT department. Downloaded software may create conflicts with existing software and result in a partial or complete PC failure.
- Request for new software will be made through the IT office.
- No unapproved software shall be brought into the department and installed onto the department's computers.
- No software from the department shall be copied for personal use.
- No employees shall use the department's computer to develop software to be used outside the department.
- Any software developed on the department's time is the property of the City of Stockbridge.
- All software must be installed or uninstalled by the IT department and will be subject to review at any time.

Use of the internet

- Brief and occasional personal use of the electronic mail system or the Internet is acceptable as long as it is not excessive or inappropriate.
- Use is defined as "excessive" if it interferes with normal job functions, responsiveness, or the ability to perform daily job activities. Electronic communication should not be used to solicit or sell products or services that are unrelated to the City's business; distract, intimidate, or harass coworkers or third parties; or disrupt the workplace.
- Employees should understand that sites visited, number of times visited, and total time connected to each site are maintained and are subject to review.

Security

- Employees of the City of Stockbridge that need to access the department's computers have an individual password that allows them to access the system.
- An employee may not share or offer the use of his or her password so that anyone else may gain access to the system.
- Unauthorized use of another employee's password is prohibited.
- No internet connection shall be installed in City facilities unless first reported and approved by the IT Department.
- All technology projects that involve internet/intranet usage shall first be reported and approved by the IT Department.

Inappropriate Use of Resources

- Any types of hacking, exploration, invasions of privacy, trespassing or other network compromises are prohibited. Excessive utilization of computer resources is prohibited. No one may deliberately attempt to degrade performance of a computer system on the Internet or to deprive authorized personnel of resources or access to any computer system. Deliberate, unauthorized excessive use of these services will be construed as an attempt to deprive others of resources.

Policy Statement for Internet/Intranet Browser(s)

- The Internet is to be used to further the City's mission, to provide effective service of the highest quality to the City's customers and staff, and to support other direct job-related purposes.
- Department Heads have the discretion to work with employees to determine the appropriateness of using the Internet for professional or personal activities.
- The various modes of Internet/Intranet access are City resources and are provided as business tools to employees who may use them for research, professional development, and work-related communications.
- Employees are individually liable for any and all damages incurred as a result of violating City security policy, copyright, and licensing agreements.
- All City policies and procedures apply to employees' conduct on the Internet, especially, but not exclusively, relating to intellectual property, confidentiality, City information dissemination, standards of conduct, misuse of City resources, anti-harassment, and information and data security.
- Employees should not bring personal computers to the workplace or connect them to City electronic systems unless expressly permitted to do so by the City.

- Violation of this policy, or failure to permit an inspection of any device covered by this policy, shall result in disciplinary action, up to and possibly including immediate termination of employment. In addition, the employee may face both civil and criminal liability from the City or from individuals whose rights are harmed by the violation.